CLAIMS

What is claimed is:

1. A method for communicating IPSec tunnel packets with compressed inner headers comprising:

storing an inner IP header and an inner protocol header from an initial IPSec tunnel packet in a context sub-table at a destination tunnel device;

for a subsequent IPSec tunnel packet, generating at the source tunnel device a compressed inner header from the inner protocol header of the subsequent IPSec tunnel packet;

performing a operation on at least one of the compressed inner header, a payload field and a padding field of the subsequent IPSec tunnel packet to generate an encapsulated portion; and

replacing at least one of the inner IP header, the inner protocol header, the payload field and the padding field of the subsequent IPSec tunnel packet with the encapsulated portion to generate an IPSec tunnel packet with compressed inner headers.

2. The method as claimed in claim 1 wherein the IPSec tunnel packet with compressed inner headers includes a tunnel header, an IPSec header, the encapsulated portion, and an authentication code, the method further comprising:

at the destination tunnel device, identifying a security association database entry for the tunnel using a security policy index number in the IPSec header;

at the destination tunnel device, decrypting the encapsulated portion to determine at least one of the compressed inner protocol header and the padding field, the padding field including a context sub-table identifier to identifies a context sub-table associated with the security association database entry;

at the destination tunnel device, retrieving at least one of the inner IP header and the inner protocol header for the subsequent IPSec tunnel packet from the context sub-table; and

recreating the subsequent IPSec tunnel packet using the inner IP header and inner protocol header retrieved from the context sub-table.

3. The method as claimed in claim 2 wherein generating the compressed inner header comprises comparing the inner protocol header with an inner protocol header of a prior IPSec tunnel packet with full inner headers.

4. The method as claimed in claim 3 wherein the generating the compressed inner header comprises generating a status field to indicate fields of the inner protocol header that have changed from the prior IPSec tunnel packet.

5. The method as claimed in claim 4 further comprising updating the inner protocol header in the context sub-table based on information in the compressed inner header, and wherein replacing comprises replacing the compressed inner header with the inner IP header retrieved from the context sub-table and the updated inner protocol header to recreate the IPSec tunnel packet with full inner headers.

6. A method for communicating IPSec tunnel packets with compressed inner headers comprising:

generating a compressed inner header from an inner protocol header of an IPSec tunnel packet with full inner headers;

performing an operation on at least one of the compressed inner header, a payload field and a padding field of the IPSec tunnel packet to generate an encapsulated portion; and

replacing at least one of an inner IP header, the inner protocol header, the payload field and the padding field of the IPSec tunnel packet with the encapsulated portion to generate an IPSec tunnel packet with compressed inner headers.

7. The method as claimed in claim 6 further comprising:

performing a second operation on the encapsulated portion of the IPSec tunnel packet with compressed inner headers to determine the compressed inner protocol header and the padding field, the padding field including a context sub-table identifier to identify a context sub-table;

retrieving the inner IP header and the inner protocol header for the IPSec tunnel packet from the context sub-table; and

recreating the IPSec tunnel packet with full inner headers using the IP header and inner protocol header retrieved from the context sub-table.

8. The method as claimed in claim 6 wherein generating the compressed inner header comprises comparing the inner protocol header with an inner protocol header of a prior IPSec tunnel packet with full inner headers.

9. The method as claimed in claim 8 wherein the IPSec data packet with full inner headers has inner headers including the inner protocol header and an inner IP header, and wherein generating the compressed inner header includes refraining from including information from the inner IP header.

10. The method as claimed in claim 8 wherein the generating the compressed inner header comprises generating a status field to indicate fields of the inner protocol header that have changed from the prior IPSec tunnel packet.

11. The method as claimed in claim 8 wherein the generating the compressed inner header comprises including a generation data field in the compressed inner header.

12. The method as claimed in claim 6 wherein performing the operation comprises performing either an encryption operation or an authentication operation on the compressed inner header, the payload field and the padding field to generate the encapsulated portion.

13. The method as claimed in claim 6 wherein performing the operation comprises adding bits to the padding field prior to performing either the encryption operation or the authentication operation.

14. The method as claimed in claim 7 wherein performing the second operation on the encapsulated portion comprises either decrypting or authenticating the encapsulated portion.

15. The method as claimed in claim 7 wherein recreating the IPSec tunnel packet with full inner headers comprises replacing the compressed inner header with the inner IP header retrieved from the context sub-table and an updated inner protocol header to recreate the IPSec tunnel packet with full inner headers, and

wherein generating the compressed inner header, performing the operation, and replacing the inner IP header are performed at a source tunnel device, and wherein performing the second operation on the encapsulated portion, retrieving, and replacing the compressed inner header are performed at a destination tunnel device.

16. The method as claimed in claim 15 further comprising:

sending an initial IPSec tunnel packet with full inner headers from the source tunnel device to the destination tunnel device; and

storing an inner IP header and an inner protocol header of the initial IPSec tunnel packet in the context sub-table at the destination tunnel device.

17. The method as claimed in claim 16 further comprising:

adding a tunnel header, an IPSec header, and an authentication code to the encapsulated portion; and

sending the IPSec tunnel packet with compressed inner headers from the source tunnel device to the destination tunnel device.

18. The method as claimed in claim 7 further comprising reading a portion of a security policy index number contained in an IPSec header to determine when an IPSec tunnel packet received at a destination tunnel device has compressed inner headers.

19. The method as claimed in claim 18 wherein reading the portion of the security policy index number further comprises reading the portion of the security policy index number to determine when the IPSec tunnel packet with compressed inner headers is a TCP type packet or a non-TCP type packet.

20. The method as claimed in claim 7 further comprising reading a portion of a security policy index number contained in the IPSec header to identify a key for use in performing a security operation on the encapsulated portion of the IPSec tunnel packet with compressed inner headers.

21. The method as claimed in claim 7 further comprising reading a portion of a security policy index number contained in the IPSec header to identify a security association database entry for an IPSec tunnel between a source tunnel device and a destination tunnel device, the security association database entry identifying a key for performing a security operation on the encapsulated portion.

22. The method as claimed in claim 21 wherein the context sub-table is one of a plurality of context sub-tables associated with the security association database entry, each context sub-table of the plurality being associated with a subnet destination tunnel device beyond the destination tunnel device.

23. The method as claimed in claim 7 further comprising updating the inner protocol header stored in the context sub-table based on information in the compressed inner header, and wherein replacing comprises replacing the compressed inner header with the inner IP header retrieved from the context sub-table and the updated inner protocol header to recreate the IPSec tunnel packet with full inner headers.

24. The method as claimed in claim 7 further comprises reading a tunnel header at a destination tunnel device to determine whether the IPSec tunnel packet with compressed headers implements an encapsulating security protocol (ESP) or an authentication header (AH) protocol, and

wherein the security operation includes a decryption when the ESP is implemented, and the security operation includes an authentication when the AH protocol is implemented.

25. The method as claimed in claim 24 further comprising:

reading a portion of a security policy index number contained in the IPSec header to identify a security association database entry for an IPSec tunnel between the source tunnel device and the destination tunnel device, the security association database entry including a flag to indicate when the encapsulated portion is encrypted; and

refraining from performing the decrypting at the destination tunnel device when the flag indicates encryption has not been performed on the encapsulated portion.

26. A tunnel device for communicating IPSec tunnel packets with compressed inner headers, the tunnel device comprising:

an inner header compressor to generate a compressed inner header from an inner protocol header of an IPSec tunnel packet with full inner headers;

a security processor to perform a security operation on the compressed inner header, a payload field and a padding field of the IPSec tunnel packet to generate an encapsulated portion; and

an IP packet processor to replace an inner IP header, the inner protocol header, the payload field and the padding field of the IPSec tunnel packet with the encapsulated portion to generate an IPSec tunnel packet with compressed inner headers.

27. The tunnel device as claimed in claim 26 wherein inner header compressor compares the inner protocol header with an inner protocol header of a prior IPSec tunnel packet with full inner headers.

28. The tunnel device as claimed in claim 27 wherein the IPSec data packet with full inner headers has inner headers including the inner protocol header and an inner IP header, and wherein the inner header compressor generating the compressed inner header refrains from including information from the inner IP header.

29. The tunnel device as claimed in claim 28 wherein the inner header compressor generating the compressed inner header generates a status field to indicate fields of the inner protocol header that have changed from the prior IPSec tunnel packet.

30. The tunnel device as claimed in claim 29 wherein a second tunnel device performs a security operation on the encapsulated portion of the IPSec tunnel packet with compressed inner headers to determine the compressed inner protocol header and the padding field, the padding field including a context sub-table identifier to identify a context sub-table, retrieves the inner IP header and the inner protocol header for the IPSec tunnel packet from the context sub-table, and recreates the IPSec tunnel packet with full inner headers using the IP header and inner protocol header retrieved from the context sub-table.

31. A computer readable medium having program instructions stored thereon for performing a method of communicating IPSec tunnel packets with compressed headers when executed within a digital processing device, the method comprising:

generating a compressed inner header from an inner protocol header of an IPSec tunnel packet with full inner headers;

performing a security operation on the compressed inner header, a payload field and a padding field of the IPSec tunnel packet to generate an encapsulated portion; and

replacing an inner IP header, the inner protocol header, the payload field and the padding field of the IPSec tunnel packet with the encapsulated portion to generate an IPSec tunnel packet with compressed inner headers.

32. The computer readable medium as claimed in claim 31 wherein generating the compressed inner header comprises comparing the inner protocol header with an inner protocol header of a prior IPSec tunnel packet with full inner headers.

33. The computer readable medium as claimed in claim 32 wherein the IPSec data packet with full inner headers has inner headers including the inner protocol header and an inner IP header, and wherein generating the compressed inner header refrains from including information from the inner IP header.

34. The computer readable medium as claimed in claim 33 wherein the generating the compressed inner header comprises generating a status field to indicate fields of the inner protocol header that have changed from the prior IPSec tunnel packet.

35. The computer readable medium as claimed in claim 34 wherein the programming instructions further comprise instructions for performing for the method which further comprise:

performing a security operation on the encapsulated portion of the IPSec tunnel packet with compressed inner headers to determine the compressed inner protocol header and the padding field, the padding field including a context sub-table identifier to identify a context sub-table;

retrieving the inner IP header and the inner protocol header for the IPSec tunnel packet from the context sub-table; and

recreating the IPSec tunnel packet with full inner headers using the IP header and inner protocol header retrieved from the context sub-table.

36. The computer readable medium as claimed in claim 35 wherein recreating the IPSec tunnel packet with full inner headers comprises replacing the compressed inner header with the inner IP header retrieved from the context sub-table and an updated inner protocol header to recreate the IPSec tunnel packet with full inner headers, and

wherein generating the compressed inner header, performing the security operation, and replacing the inner IP header are performed at a source tunnel device, and wherein performing the security operation on the encapsulated portion, retrieving, and replacing the compressed inner header are performed at a destination tunnel device.

37. The computer readable medium as claimed in claim 36 wherein the programming instructions further comprise instructions for performing for the method which further comprise:

sending an initial IPSec tunnel packet with full inner headers from the source tunnel device to the destination tunnel device; and

storing an inner IP header and an inner protocol header of the initial IPSec tunnel packet in the context sub-table at the destination tunnel device.

38. The computer readable medium as claimed in claim 36 wherein the programming instructions further comprise instructions for performing for the method which further comprise updating the inner protocol header in the context sub-table based on information in the compressed inner header, and wherein replacing comprises replacing the compressed inner header with the inner IP header retrieved from the context sub-table and the updated inner protocol header to recreate the IPSec tunnel packet with full inner headers.